

BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554

EB Docket No. 06-36

**ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION**

Annual 64.2009(e) CPNI Certification for 2007

Date filed: September 25, 2008

Name of company covered by this certification: USA Datanet Wholesale, Inc.

Form 499 Filer ID: 826668

Name of signatory: Richard Popper

Title of signatory: Chief Operating Officer

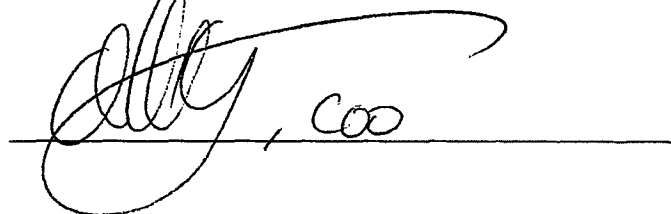
I, Richard Popper, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules, to the extent those procedures apply to the information we obtain from our carrier customers. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system or at the Commission) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



## **USA DATANET WHOLESALE, INC.** **STATEMENT OF CPNI PROCEDURES**

USA Datanet Wholesale, Inc. ("USADW") takes the protection of CPNI seriously. USADW has received legal counsel in this area and protects the confidentiality of its carrier customers' information. USADW receives *limited information* from its carrier customers and uses that information solely to perform the telecommunications services, for billing purposes and in response to legal process. It does not use this information for marketing purposes to its carrier customers or any end users. USADW has no end user customers.

### **Duty to Protect CPNI**

We recognize a duty to protect customer CPNI if we possess CPNI. To the extent we obtain CPNI, we may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

1. Administrative use: We may use CPNI to *initiate, render, bill and collect* for communications services.
2. Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
3. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

### **Our Own Use Of CPNI**

At this time, we do not use CPNI to market to our carrier customers. However, at a later date, we may use CPNI to provide or market services to our existing customers. We understand that we are required to obtain customer approval prior to using CPNI in certain ways, and will ensure compliance if we seek to use CPNI to market services.

We do not share CPNI with any affiliates or other third parties for marketing purposes.

## **Authenticating Customers Before Disclosing CPNI**

We understand that we are required to objectively determine that our customers are who they say they are before disclosing CPNI to them.

### **Telephone**

We do not release *call detail information*, or information relating to the transmission of specific telephone calls over the telephone. Our carrier customers can only access this information through a secure, authenticated network.

### **In-Person Authentication**

We do not release CPNI through in-person visits. Our carrier customers can only access this information through a secure, authenticated network.

### **Mail**

If the customer requests CPNI through regular mail, or if the customer cannot comply with the authentication method above, we send the requested information to the customer's address of record only.

### **Online Access**

We password protect online access to CPNI. USADW's carrier customers can access the Information solely through a secure online network that requires authentication. USADW utilizes a third-party billing company, Telebill, which has access to the billing CDR for billing purposes only. Telebill is a small company that is aware of the Commission's CPNI regulations and has safeguards in place to protect the Information. The CDR that is provided to our carrier customers (so that they may bill their customers and reconcile their invoices against their own CDR) is available to our customers only through a secure FTP site provided by Telebill. Customers access the FTP site using a unique login and password combination which is provided to them by USADW staff. USADW, in turn, gives that information to Telebill, which sets up the unique FTP site. USADW will only provide the login information to previously authorized personnel, as submitted to USADW by our customers.

## **Training And Discipline**

We have trained applicable employees regarding the company's CPNI policies. Employees will have an annual retraining to ensure that they understand the company's CPNI policies and any updates to those policies. New employees who will have access to CPNI will be trained when they join the company, and then attend the regularly-scheduled retraining sessions. Employees are subject to disciplinary action for failure to abide by our requirements.

## **Record-Keeping**

We maintain records of discovered CPNI breaches, notifications to law enforcement regarding breaches, and any responses from law enforcement regarding those breaches, in our files for at least two (2) years.

### **Notification Of Account Changes**

We understand that we are required to notify customers when changes have been made to passwords, customer responses to back-up means of authentication, online accounts, or addresses of record by mailing a notification to the account address of record.

We do not reveal the changed account data in the notification.

### **Unauthorized Disclosure Of CPNI**


We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at <http://www.fcc.gov/eb/CPNI/> to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

Records relating to such notifications are kept in accordance with our record-keeping policies. These records include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Signed



A handwritten signature in black ink, appearing to read "J. J. Coe", is written over a horizontal line.